A Proof-theoretic Trust and Reputation Model for VANET

Giuseppe Primiero, Franco Raimondi, Taolue Chen and Rajagopal Nagarajan
Department of Computer Science,
Middlesex University London, United Kingdom
Email: G.Primiero—F.Raimondi—T.Chen—R.Nagarajan@mdx.ac.uk

Abstract—Vehicular Ad Hoc Networks (VANETs) are an important component of intelligent transportation systems, which are set to become part of global transportation infrastructure in the near future. In the context of such networks, security requirements need to rely on a combination of reputation of communicating agents and trust relations over the messaging framework. This is crucial in order to maintain dynamic and safe behaviour under all circumstances. Formal correctness, resolution of contradictions and proven safety of transitive operations in the presence of reputation and trust within the infrastructure remain mostly unexplored issues. This could lead to potentially disastrous situations, putting lives at risk. In this paper we provide a proof-theoretic interpretation of a reputation and trust model for VANET. This allows for formal verification through translation into the Coq proof assistant, and can guarantee consistency of messaging protocols and security of transitive transmissions.

1. Introduction

Vehicular Ad Hoc Networks (VANETs) consist of vehicles and roadside unit networks created to enhance transportation systems through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. VANET services include: vehicle and road safety services, which target characteristics like the decrease of traffic accidents and loss of life to vehicle occupants; traffic efficiency and management services, which aim to improve traffic flow, traffic coordination, and to provide local and map information; information and entertainment services, to provide multimedia data transfer and global Internet access, [7].

Due to their distributed and dynamic nature, such networks are open to several types of threats, including false message propagation. Trust and reputation are among the most used concepts to ensure integrity, reliability and safety of services. Several methods have been implemented in VANETs to manage trust, see [14] for a recent overview. Trust models in VANETs differ in accordance to the main object of the model: entity-centric [9], [4], data-centric [12], [8] and combined [16]. The work in [15] offers an analysis that accounts for reputation as a characteristic of message forwarding among vehicles, drivers and other agents: reputation of these agents is based on a descriptive ontology and is used to provide feedback in the system. An overview of the issues related to trust in fixed and mobile ad hoc networks is given in [17], while other approaches for trustworthiness and reputation in ad hoc mobile networks are presented, for example, in [3], [2].

In most of these models, the analysis relies on simulations. However, such simulations cannot guarantee the absence of unpredictable and unsafe behaviours. Since VANETs are meant to include safety and emergency messages, more reliable methods are essential. The only method to produce exhaustive safety control is through formal verification, but unfortunately none of the current trust and reputation models seem to have focused on a formal correctness requirement to ensure that the protocols are verifiable. Formal approaches to VANET include the work in [6] for the verification of a congestion control protocol using the model checker PRISM to investigate its correctness and effectiveness; verification of privacy and authentication using the AVISPA tool in [1]; verification of the TESLA authentication protocol [5] using Petri nets. Such approaches are few and far apart. Moreover, they do not focus explicitly on trust or reputation and they are all based on model checking. Other formal verification techniques like theorem proving seem to have been ignored so far. Moreover, an additional problem, i.e., ensuring that safety is preserved over transitive operations, remains unexplored. In particular, the problem of a message passing over from vehicle $v_i$ to $v_j$ and from $v_j$ to $v_k$ illustrate the need to guarantee that for each such transition security and safety properties are preserved.

The present paper addresses both problems mentioned above. In Section 2, we formulate a proof-theoretic translation of the trust and reputation model for VANET given in [15] with an extension of the natural deduction calculus (un)SecureND from [10]. The aim is, first of all, to show that the trust properties instantiated through our calculus faithfully reflect those in a VANET network; accordingly, non-trustworthy interactions can be identified through a proof-checking method. On a higher level, the model offered by (un)SecureND has been proven formally correct through its translation to a Coq library. As such, the present translation guarantees a similar property for the whole VANET model. Thanks to the structural properties of our calculus, we show how transitive message passing operations, in the form of instances of a cut rule, are guaranteed safe via applying a normalisation result. In other
words, we are able to qualify as safe a message passing operation through any number of vehicles by checking at each interaction that consistency is preserved. In Section 3, we illustrate protocols for handshaking, recipient selection and message passing based on reputation. In Section 4, we give a reputation model based on an evaluation of parametrised feedback messages, in view of a temporal measure and a ranking of the relevant service characteristic of each message.

2. (un)SecureND

Recall that (un)SecureND is a natural deduction calculus defining trust, mistrust and distrust protocols introduced in [11] and extended in [10] with a negation connective. Here we provide a slightly modified version, adapted for a VANET network. In particular, in the present version we introduce: contexts as sets of sets; formulas with multiple indices to account for service and message numbers; ranking on service characteristics. We start with introducing the language of the logic:

Definition 1 (Syntax of (un)SecureND).

\[ A := \{V, R\} \]
\[ V := \{v_1, \ldots, v_n\} \]
\[ R := \{rsu_1, \ldots, rsu_m\} \]
\[ S := \{S_1, \ldots, S_n\} \]
\[ C := \{C_{\pi}^{S_i}, \ldots, C_{\pi}^{S_n}\} \]
\[ \phi_{A, C_j} := a_{A, C_j} \mid \neg \phi_{A, i,j} \mid \phi_{A, i,j} \rightarrow \phi_{A, k,l} \mid \phi_{A, i,j} \wedge \phi_{A, k,l} \mid \phi_{A, i,j} \vee \phi_{A, k,l} \mid \bot \mid \text{Read}(\phi_{A, C_i}) \mid \text{Write}(\phi_{A, C_i}) \mid \text{Trust}(\phi_{A, C_i}) \]
\[ \Gamma_A := \phi_{A, i,j} \mid \phi_{A, i,j} < \phi_{A, k,l} \mid \Gamma_A : \phi_{A, i,j} \]

\[ A \] is the set of agents issuing messages containing vehicles \( V \) and roadside units (RSUs) \( R \). Below we will focus in particular on V2V communication, without loss of generality. The order \( \prec \) between agents is a reputation order, defined below in Section 4. \( S \) denotes a set of services. \( C \) denotes a set of service characteristics, with each element \( C_{\pi}^{S_i} \) denoting the set of \( n \) characteristics of service \( S_i \). We assume, here and throughout, that characteristics \( C_{\pi}^{S_i} \) of services for each service \( S_i \) are associated with an order \( \leq \), so are given as posets, and the ordering \( \leq \) is used to order messages below in Definition 4. Note that for two characteristics \( C_{\pi}^{S_i} \) and \( C_{\pi}^{S_j} \) respectively with \( i \neq j \), there is no order between them.

Messages are boolean formulae, closed under connectives and including \( \bot \) to express conflicts. Messages are signed by agents generating them and by service and characteristic identifiers: \( \phi_{A, C_j} \) expresses a message \( \phi \) about characteristic \( C_j \) of service \( S_k \) generated by vehicle \( v_i \). To simplify, we often abbreviate this notation as \( \phi_{k,j} \). When required, we will refer to a set of messages about service \( S_k \) and characteristic \( C_j \) from vehicle \( v_i \) as \( M_{S_k,C_j}^{v_i} \); this notation can be further generalised to a whole set of vehicles \( \{v_1, \ldots, v_k\} \subseteq A \). A profile for vehicle \( v_i \), denoted as \( \Gamma^{v_i} \), is the current list of all messages collected by \( v_i \) from available sensors, other agents and networks. For the present purposes, information from networks will be indexed at their first receiving vehicle, so as not to add networks as separate agents. For example, a vehicle profile \( \Gamma^{v_j} \) receives a message \( \phi_{j,k} \) about service \( S_j = \text{weather} \) and characteristic \( C_k = \text{temperature} \) stating \( \phi = (\text{temp} \geq 5^\circ \text{C}) \). We can now define the notion of judgement in the language:

Definition 2 (Judgements). A judgement \( \Gamma^{v_j} \vdash \phi_{i,k}^{v_j} \) states that a message \( \phi \) about service \( i \) and characteristic \( k \) signed from agent \( v_j \) is validly accessed at step \( a \geq 0 \) under the profile of agent \( v_i \).

Definition 3 (Validity). A judgement \( \vdash \phi_{i,k}^{v_j} \) says that a message \( \phi \) about service \( i \) and characteristic \( k \) signed from vehicle \( v_j \) holds for any vehicle’s profile at step \( a \).

Messages satisfy a ranking based on characteristics:

Definition 4. We define an order \( \leq \) between messages such that \( \phi_{i,k}^{v_j} < \phi_{l,j}^{v_j} \) holds if \( C_k \leq C_l \) for a vehicle \( v_j \).

Therefore the order relation \( \leq \) between service characteristics induces validity under profile: if a characteristic \( k \) is essential to another characteristic \( l \) with respect to a service \( i \) for a vehicle \( v_j \), then \( v_j \) will be required to obtain a value for \( k \) in order to validly access a value for \( l \). An example of such order between characteristics could be as follows: under the service weather, \( C_k = \text{humidity} \) and \( C_l = \text{precipitation} – \text{forecast} \), where the former characteristic is essential to determine the latter.

A valid vehicle profile meets all the requirements and conflicts clauses of all service messages that the vehicle receives. A conflict is generated by two contradictory messages, and the profile is valid when such conflicts are avoided; a requirement is the need of a given value for some service and requirement, and a valid profile contains all such required values. We use \( \text{profile} \) as a typing term to denote a sets of formulas valid for a vehicle. Profile construction by service messages requirements is defined by rules from Figure 1. We start by declaring an empty profile to be valid (base case); by Message Insertion, a valid message can be inserted in a vehicle profile; by Requirement Insertion, a profile can be extended by satisfied service requirements; by Profile Extension, if a message holds in an empty profile, it can be added to an existing profile. In this syntax, the construction of two vehicle profiles \( \Gamma^{v_i}; \Gamma^{v_j} \) : \text{profile} will typically denote the existence of an active communication channel between vehicles \( v_i, v_j \).

2.1. Rules for message construction

The operational rules in Figure 2 formulate compositionality of messages. The rule \( \text{Atom} \) establishes that a vehicle and a communication channel between vehicles can qualify a message as valid if all its requirements are satisfied. Rule \( \bot \) expresses that contradictory messages imply access to their negation. Rule \( \wedge \text{-I} \) allows to compose message originating from different vehicles; by rule \( \wedge \text{-E} \), decomposition is valid for the channel obtained by the vehicles
from which the messages originate. Rule \(\lor\)-I says that a channel of two vehicles profiles can access any message produced from each of the composing vehicle profiles; by the elimination rule \(\lor\)-E, each message consistently inferred by each individual vehicle profile can also be executed under the channel between the profiles of the two vehicles. Rule \(\to\)-Introduction expresses inference of a message from a channel as inference between messages (Deduction Theorem); its elimination through rule \(\to\)-E allows to recover such inference as profile extension (Modus Ponens).

### 2.2. Access Rules

In Figure 3 we present the access rules on messages. These allow a vehicle to act on messages received from another vehicle. Rule \(\neg\)-distribution expresses profile consistency: if a vehicle profile does not allow inferring a message \(\phi_{i,j}\), then it allows inferring any other message whose requirements do not include \(\phi_{i,j}\). Rule \(\text{read}\) says that from any consistent vehicle profile a message can be read provided its requirements are satisfied (if any). Rule \(\text{trust}\) works as an elimination rule for \(\text{read}\): it says that if a message is received by a vehicle and it preserves its profile consistency, then it can be trusted. Rule \(\text{write}\) works as an elimination rule for \(\text{trust}\): it says that a message readable and trustable by a vehicle can be broadcast. Rule \(\text{exec}\) says that every message consistently received by a vehicle is valid in it. The rule \(\text{MTrust-I}\) says that currently held message conflicting with a newly arrived message is mistrusted, i.e., removed from the current vehicle profile until none of its consequences are included; the corresponding \(\text{MTrust-E}\) elimination allows to trust any message consistent with the conflict resolution by removal of the mistrusted message in the vehicle profile, including any required dependency: this is expressed by the side condition that requires checking with any other vehicle with higher reputation than the sender of the original message. The side condition can be modified at will, e.g., to design a protocol that will restore previous information if a sufficient number of other vehicles with higher reputation support it. \(\text{mistrust}\) is a flag for facilitating removal of messages present in the vehicle profile conflicting in view of incoming new information.

### 2.3. Structural Rules

Structural rules hold with restrictions for (un)\text{SecureND}, see Figure 4. As a result, the system qualifies as substructural, see for instance [13]. Weakening is constrained by an instance of \(\text{trust}\): it says that valid information is preserved under a vehicle’s profile extension, assuming the latter is provably consistent. Contraction is constrained by preservation of ordering: it says that removing identical messages from a vehicle’s profile is admissible, with the constraint that the copy from the vehicle with higher reputation is preserved. Exchange is constrained by dependency: it says that reorder of messages is admissible if there is no involved dependency between them. Finally, the \(\text{Cut}\) rule expresses validity under a vehicle’s profile extension: if a message \(\phi_{i,j}\) is valid for vehicle \(v_i\) and after messaging it to \(v_j\) the latter can infer \(\phi_{i,k}\), then \(v_i\) can infer \(\phi_{i,k}\) by setting a message protocol with \(v_j\).

**Theorem 1** (Normalisation). Any message \(\phi_{i,k}\) valid for a channel \(v_i, v_j\) and obtained by an occurrence \(c\) of the \(\text{Cut}\) rule can be validated without \(c\) using only \(\text{trust}\).

**Proof.** By induction on the derivation \(D\) which is the redex of the cut-elimination. Assuming \(c\) is the only Cut rule and it is the last inference rule of the redex, the derivation \(D’\) which is the contractum of the cut-elimination contains a descendent of the cut obtained by an instance of Weakening under trust. Because the formula obtained by the cut is, by hypothesis, derivable from the weaker protocol, it will also be derivable from the weaker and the stronger protocol together. When \(c\) is not the last inference rule of the redex, then the descendent of the cut will admit all similar Weakening preserving the one occurring in the cut; those imports by Weakening will occur also in the contractum of the cut rule and can be traced back up to the one formulation of the import that occurs in the cut rule.

Normalisation justifies a safety property of our trust and reputation model over transitive transmissions: for each vehicle \(v_i, v_j, v_k\), if \(v_k\) holds information \(\phi_{i,j}\) and this information is passed to \(v_j\), then every valid message derived from \(\phi_{i,j}\) by \(v_k\) can be inferred by \(v_j\) assuming the consistency (by trust) of its profile with that of \(v_k\); similarly now, \(v_j\) can pass \(\phi_{i,j}\) to \(v_i\), and the latter can infer from there, assuming its profile is consistent with those of \(v_j, v_k\).
3. Opportunistic Forwarding

In this section we present the algorithm and exemplify derivations for handshaking and opportunistic message forwarding protocols. The algorithm consists of two parts: it first selects a recipient for the communication according to a reputation model; then it implements message forwarding if consistency is guaranteed by trust. The pseudo-code of the reputation model; then it implements message forwarding if required; Here the idea is as follows: after $v_i$ broadcasts a ‘hello’ message, both $v_k, v_j$ receive and accept the message; at this stage a recipient is selected on the basis of the reputation order between $v_k$ and $v_j$, so that a new profile is built out of $v_i$ and the higher of the two recipients, thus modelling a communication channel.

In Figure 7, we present an example derivation of the recipient selection protocol. Here the idea is as follows: after $v_i$ broadcasts a ‘hello’ message, both $v_k, v_j$ receive and accept the message; at this stage a recipient is selected on the basis of the reputation order between $v_k$ and $v_j$, so that a new profile is built out of $v_i$ and the higher of the two recipients, thus modelling a communication channel.

In Figure 8, we present an example derivation modelling a message passing protocol (without mistrust). Here Service 2 is a service of any kind. By the first premise in MP, the Handshaking Protocol is guaranteed terminating, including the Recipient Selection protocol if required; $v_k$ then reads a message issued by $v_i$, checks for validity in its own profile through an application of trust, and if this check is passed the message is forwarded.

4. Reputation Model

In this section we illustrate the definition of the order relation $\prec$ to formalise the reputation model across vehicles, implementing the system as in [15]. The main idea of
We proceed now with the formalisation of this model. of messages of the former is higher than that of the latter. Each vehicle and service, a vehicle will result having higher reputation than another (with respect to a set of messages) if it received about that service characteristic, weighted by the relevance of that characteristic to the current user’s profile. We can now generalise to the set of all feedback on a service. The perception of vehicle $v_j$ for a message $\phi_{i,j}$, for all $v_j, v_i \in A$ is the sum of elements of the feedback set over that formula, weighted by the step of the derivation at which it is obtained:

$$AP^{v_j}(\phi_{i,j}) = \sum_{FS^{v_j}(\phi_{i,j})} (s(\psi_{i,k} \in FS^{v_j}(\phi_{i,k})))$$

Intuitively, the value of $s$ at each step of each derivation leading to each formula in the feedback set of a vehicle to a given service and characteristic is summed up to provide a value that increases linearly to reflect a step value for a time function. The value of $AP^{v_j}(\phi_{i,j})$ will reflect the aggregation of all the feedback provided on each characteristics of a given service.

We can now generalise to the set of all feedback on a characteristic for a given service, remembering that these are given in a preorder so that the position of the characteristic in that order is mapped into an integer:

$$AP^{v_j}(\mathcal{M}^d_{S_i,C_k}) = \sum_{FS^{v_j}(\phi_{i,k})} (1 - r(C_k)(s(\psi_{i,k} \in FS^{v_j}(\phi_{i,k}))))$$

Using the vehicle’s perception of characteristic set, we can define the order of reputation with respect to services.
Definition 8 (Reputation). \( \forall v_i, v_j \in V, S_i \in S, v_i < v_j \iff AP^{v_i}(M_{S_i,C_i}^{\delta}) > AP^{v_j}(M_{S_j,C_j}^{\delta}) \).

5. Conclusions

In this paper we have formulated a proof-theory for trust and reputation in VANETs. Our language is modelled on the logic \((\text{un})\text{SecureND}\), including an explicit trust function on formulas to guarantee consistency check at each retrieval step (after a read function), before forwarding is granted for a package (by a write function). Forwarding is modelled in an opportunistic fashion, selecting receivers on the basis of their reputation ranking. Trust on forwarding also guarantees correctness on transitive transmissions. Moreover, reputation is used to implement the resolution protocol for restoring information after removing previously stored data. Several improvements for the algorithm are possible, including majority selection on opportunistic forwarding (instead of consensus) and separate ordering for vehicles and RSUs. Validation of the system is obtained by implementation of the \((\text{un})\text{SecureND}\) calculus as a large inductive type in the Coq proof assistant. The development is available at https://github.com/gprimiero/SecureNDC. A characteristic of the logic \((\text{un})\text{SecureND}\) is its substructural nature, which in future work can be exploited to investigate cases of strengthened and limited resource redundancy for fault tolerance and source shuffling for security. Other applications of negative trust can be investigated to distinguish between malevolent and simply unsuccessful sources.

Acknowledgement. Taolue Chen is partially supported by UK EPSRC grant (EP/P00430X/1) and European CHIST-ERA project SUCCESS.

References


